


# Exhibit 2

 An official website of the United States government  
[Here's how you know](#)



## Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, January 28, 2021

# Emotet Botnet Disrupted in International Cyber Operation

## **Emotet Malware Infected More than 1.6 Million Victim Computers and Caused Hundreds of Millions of Dollars in Damage Worldwide**

The Justice Department today announced its participation in a multinational operation involving actions in the United States, Canada, France, Germany, the Netherlands, and the United Kingdom to disrupt and take down the infrastructure of the malware and botnet known as Emotet. Additionally, officials in Lithuania, Sweden, and Ukraine assisted in this major cyber investigative action.

"The Emotet malware and botnet infected hundreds of thousands of computers throughout the United States, including our critical infrastructure, and caused millions of dollars in damage to victims worldwide," said Acting Deputy Attorney General John Carlin. "Cyber criminals will not escape justice regardless of where they operate. Working with public and private partners around the world we will relentlessly pursue them while using the full arsenal of tools at our disposal to disrupt their threats and prosecute those responsible."

According to an unsealed search warrant affidavit, Emotet is a family of malware that targets critical industries worldwide, including banking, e-commerce, healthcare, academia, government, and technology. Emotet malware primarily infects victim computers through spam email messages containing malicious attachments or hyperlinks. Emails were designed to appear to come from a legitimate source or someone in the recipient's contact list. Once it has infected a victim computer, Emotet can deliver additional malware to the infected computer, such as ransomware or malware that steals financial credentials. Ransomware, in particular, has increased in scope and severity in the past year, harming businesses, healthcare providers, and government agencies even as the country has struggled to respond to the pandemic.

"The coordinated disruption of Emotet was a great success for the FBI and our international partners," said FBI Director Christopher Wray. "The FBI utilized sophisticated techniques, our unique legal authorities, and most importantly, our worldwide partnerships to significantly disrupt the malware. The operation is an example of how much we can achieve when we work with our international law enforcement partners to combat the cyber threat. The FBI remains committed, now more than ever, to imposing risk and consequences on cyber criminals to put an end to this type of criminal activity."

The computers infected with Emotet malware are part of a botnet (i.e., a network of compromised computers), meaning the perpetrators can remotely control all the infected computers in a coordinated manner. The owners and operators of the victim computers are typically unaware of the infection.

"Cybercrime transcends physical and political boundaries and costs U.S. citizens and businesses billions each year," said U.S. Attorney Matt Martin of the Middle District of North Carolina. "That was certainly true with Emotet. Now, more than ever, international collaboration is an imperative as we employ a technically and legally sophisticated approach to thwart cybercriminals in whatever corner of the globe they are found. This investigation will be a paradigm for effective

international law enforcement cooperation directed at global cybercrime, and we applaud the FBI and the international law enforcement partners who contributed to the effort to take down this global threat.”

According to the affidavit, in 2017, for example, the computer network of a school district in the Middle District of North Carolina was infected with the Emotet malware. The Emotet infection caused damage to the school’s computers, including but not limited to the school’s network, which was disabled for approximately two weeks. In addition, the infection caused more than \$1.4 million in losses, including but not limited to the cost of virus mitigation services and replacement computers. From 2017 to the present, there have been numerous other victims throughout North Carolina and the United States, to include computer networks of local, state, tribal, and federal governmental units, corporations, and networks related to critical infrastructure.

“The Emotet malware quickly elevated to one of the top cyber threats in the world,” said Special Agent in Charge Robert R. Wells of the FBI Charlotte Field Office. “The strong relationships with international law enforcement partners were critical to the success of this FBI investigation which began with a small North Carolina school system that did the right thing and quickly contacted their local FBI office for help.”

According to the U.S. Cybersecurity & Infrastructure Security Agency (CISA), Emotet infections have cost local, state, tribal, and territorial governments up to \$1 million per incident to remediate. More information about the malware, including technical information for organizations about how to mitigate its effects, is available from CISA here: <https://us-cert.cisa.gov/ncas/alerts/TA18-201A>.

According to the affidavit, foreign law enforcement agents, working in coordination with the FBI, gained lawful access to Emotet servers located overseas and identified the Internet Protocol addresses of approximately 1.6 million computers worldwide that appear to have been infected with Emotet malware between April 1, 2020, and Jan. 17, 2021. Of those, over 45,000 infected computers appear to have been located in the United States.

Foreign law enforcement, working in collaboration with the FBI, replaced Emotet malware on servers located in their jurisdiction with a file created by law enforcement, according to the affidavit. This was done with the intent that computers in the United States and elsewhere that were infected by the Emotet malware would download the law enforcement file during an already-programmed Emotet update. The law enforcement file prevents the administrators of the Emotet botnet from further communicating with infected computers. The law enforcement file does not remediate other malware that was already installed on the infected computer through Emotet; instead, it is designed to prevent additional malware from being installed on the infected computer by untethering the victim computer from the botnet.

The scope of this law enforcement action was limited to the information installed on infected computers by the Emotet operators and did not extend to the information of the owners and users of the computers.

According to the affidavit, in coordination with foreign law enforcement officials, FBI personnel also gained lawful access to an Emotet distribution server located overseas and identified several servers worldwide that were used to distribute the Emotet malware. These servers were typically compromised web servers belonging to what appear to be unknowing third parties. The perpetrators uploaded the Emotet malware to the servers through unauthorized software applications. Victims who clicked on spam email messages containing malicious attachments or hyperlinks would then download the initial Emotet malware file from a distribution server.

In addition, according to the affidavit, FBI personnel notified more than 20 U.S.-based hosting providers that they hosted more than 45 IP addresses that had been compromised by the perpetrators associated with the Emotet malware and botnet. FBI Legal Attachés further notified authorities in more than 50 countries that hosting providers in their respective jurisdictions hosted hundreds of IP addresses that were compromised by Emotet.

The U.S. Attorney’s Office for the Middle District of North Carolina, the FBI Charlotte Division, and the Criminal Division’s Computer Crime and Intellectual Property Section (CCIPS) conducted the operation in close cooperation with Europol and Eurojust who were an integral part of coordination and messaging, and investigators and prosecutors from several jurisdictions, including the Royal Canadian Mounted Police, France’s National Police and Judicial Court of Paris, Germany’s Federal Criminal Police and General Public Prosecutor’s Office Frankfurt/Main, Lithuanian Criminal Police Bureau, Netherlands National Police and National Public Prosecution Office, Swedish Police Authority, National Police of Ukraine and Office of the Prosecutor General of Ukraine, and the United Kingdom’s National Crime Agency

and Crown Prosecution Service. The Justice Department's Office of International Affairs and the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN) also provided significant assistance. CCIPS Senior Counsel Ryan K.J. Dickey and Assistant U.S. Attorneys Eric Iverson and Anand Ramaswamy of the Middle District of North Carolina led the U.S. efforts.

More information about the operation is available by clicking: [Eurojust](#) /[Europol](#) . In addition, the Dutch National Police have created the following website to check whether your email address has been compromised by the administrators of Emotet: <https://www.politie.nl/emocheck> .

In September 2020, FBI Director Christopher Wray announced the FBI's new strategy for countering cyber threats. The strategy focuses on imposing risk and consequences on cyber adversaries through the FBI's unique authorities, world-class capabilities, and enduring partnerships. Victims are encouraged to report the incident online with the Internet Crime Complaint Center (IC3) [www.ic3.gov](http://www.ic3.gov). For more information on ransomware prevention, visit: <https://www.ic3.gov/Home/Ransomware>.

---

**Attachment(s):**

[Download Emotet search and seizure warrant](#)

[Download Emotet application and affidavit](#)

**Topic(s):**

Cyber Crime

**Component(s):**

[Criminal Division](#)

[Criminal - Computer Crime and Intellectual Property Section](#)

[Criminal - Office of International Affairs](#)

[Federal Bureau of Investigation \(FBI\)](#)

[Office of the Deputy Attorney General](#)

[USAO - North Carolina, Middle](#)

**Press Release Number:**

21-104

*Updated January 28, 2021*



THE UNITED STATES ATTORNEY'S OFFICE  
WESTERN DISTRICT *of* WASHINGTON

[U.S. Attorneys](#) » [Western District of Washington](#) » [News](#)

Department of Justice

U.S. Attorney's Office

Western District of Washington

FOR IMMEDIATE RELEASE

Tuesday, July 7, 2020

**Citizen of Kazakhstan, known as “fxmsp,” charged with  
computer fraud, wire fraud, and conspiracy for hacking  
hundreds of corporate networks in more than 40 countries  
worldwide**

**Prolific hacker sold network access to other cybercriminals on various underground  
forums, enabling various further cyberattacks**

Seattle – An indictment was unsealed today in the Western District of Washington charging a citizen of Kazakhstan, ANDREY TURCHIN, a/k/a “fxmsp,” 37, with various federal crimes related to a prolific, financially motivated cybercrime group that hacked the computer networks of a broad array of corporate entities, educational institutions, and governments throughout the world, announced U.S. Attorney Brian T. Moran. The “fxmsp” group established persistent access, or “backdoors,” to victim networks, which they then advertised and sold to other cybercriminals subjecting victims to a variety of cyberattacks and fraud.

“Cybercrime knows no international borders, and stopping these crimes requires cooperation between an array of international partners. I commend Kazakhstan for its assistance in this investigation,” said U.S. Attorney Brian T. Moran. “I am hopeful these critical international partnerships between cybercrime investigators will lead to holding Andrey Turchin accountable in a court of law.”

“Sophisticated cybercrimes can be extremely difficult to investigate. However, by working closely with our international law enforcement partners at the UK’s National Crime Agency, along with victims, private sector security researchers and great cooperation from our international law enforcement partners in Kazakhstan, the FBI was able to disrupt Mr. Turchin and his alleged co-conspirator’s criminal intrusions,” said Raymond Duda, Special Agent in Charge FBI Seattle Field Office. “This case demonstrates the FBI’s commitment to uncover and counter cyber criminals, domestic or abroad.”

According to the five-count indictment and records on file, from at least October 2017 through the date charges were returned by a Grand Jury, in December 2018, TURCHIN and his accomplices perpetrated an ambitious hacking enterprise broadly targeting hundreds of victims across six continents, including more than 30 in the United States. Widely known in hacking circles by the moniker “fxmsp,” TURCHIN employed a collection of hacking techniques and malicious software (malware) to gain and maintain access to victim networks. For instance, he often used specially designed code to scan the Internet for open Remote Desktop Protocol (RDP) ports and conduct brute-force attacks to initially compromise victim networks. Once

inside the victim's system, he moved laterally throughout the network and deployed additional malicious code to locate and steal administrative credentials and establish persistent access. The conspirators often modified antivirus software settings to allow malware to continue to run undetected.

TURCHIN and his co-conspirators then marketed and sold the network access on various underground forums commonly frequented by hackers and cybercriminals, such as Exploit.in, fuckav.ru, Club2Card, Altenen, Blackhacker, Omerta, Sniff3r, and L33t, among others. Prices typically ranged from a couple thousand dollars to, in some cases, over a hundred thousand dollars, depending on the victim and the degree of system access and controls. Many transactions occurred through use of a broker and escrow, which allowed interested buyers to sample the network access for a limited period to test the quality and reliability of the illicit access. As has been publicly reported, the "fxmsp" group has been linked to numerous high-profile data breaches, ransomware attacks, and other cyber intrusions.

TURCHIN is charged with conspiracy to commit computer hacking, two counts of computer fraud and abuse (hacking), conspiracy to commit wire fraud, and access device fraud. Conspiracy to commit computer fraud is punishable by up to five years in prison. The two counts of computer fraud and abuse (hacking) are punishable by up to ten and five years in prison, respectively. Conspiracy to commit wire fraud is punishable by up to 20 years in prison. Access device fraud is punishable by up to ten years in prison.

The charges contained in the indictment are only allegations. A person is presumed innocent unless and until he or she is proven guilty beyond a reasonable doubt in a court of law.

The case is being investigated by the FBI Seattle Office, Cyber Crime Task Force, with the cooperation of the United Kingdom's National Crime Agency (NCA), and with assistance from the U.S. Department of Justice's Criminal Division's Office of International Affairs, the FBI Legal Attaché Offices in London and Nur-sultan, and the National Security Committee of the Republic of Kazakhstan (KNB).

The case is being prosecuted by Assistant United States Attorney Steven Masada.

[turchin\\_indictment.pdf](#)

---

**Attachment(s):**

[Download turchin\\_indictment.pdf](#)

**Topic(s):**

Cyber Crime


**Component(s):**

[USAO - Washington, Western](#)

**Contact:**

Press contact for the U.S. Attorney's Office is Communications Director Emily Langlie at (206) 553-4110 or [Emily.Langlie@usdoj.gov](mailto:Emily.Langlie@usdoj.gov).

Updated July 7, 2020

 An official website of the United States government  
[Here's how you know](#)



**Department of Justice**

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, December 5, 2019

**Russian National Charged with Decade-Long Series of Hacking and Bank Fraud  
Offenses Resulting in Tens of Millions in Losses and Second Russian National  
Charged with Involvement in Deployment of “Bugat” Malware**

**Reward of up to \$5 Million Offered for Information Leading to Arrest or Conviction**

The United States of America, through its Departments of Justice and State, and the United Kingdom, through its National Crime Agency (NCA), today announced the unsealing of criminal charges in Pittsburgh, Pennsylvania, and Lincoln, Nebraska, against Maksim V. Yakubets, aka online moniker, “aqua,” 32, of Moscow, Russia, related to two separate international computer hacking and bank fraud schemes spanning from May 2009 to the present. A second individual, Igor Turashev, 38, from Yoshkar-Ola, Russia, was also indicted in Pittsburgh for his role related to the “Bugat” malware conspiracy. The State Department, in partnership with the FBI, announced today a reward of up to \$5 million under the Transnational Organized Crime Rewards Program for information leading to the arrest and/or conviction of Yakubets. This represents the largest such reward offer for a cyber criminal to date.

Assistant Attorney General Brian A. Benczkowski of the Justice Department’s Criminal Division, U.S. Attorney Scott W. Brady for the Western District of Pennsylvania, U.S. Attorney Joseph P. Kelly for the District of Nebraska, FBI Deputy Director David Bowdich, Principal Deputy Assistant Secretary James A. Walsh of the State Department’s Bureau of International Narcotics and Law Enforcement Affairs (INL), and Director Rob Jones of the Cyber Crime Unit at the United Kingdom’s National Crime Agency (NCA) made the announcement.

“Maksim Yakubets allegedly has engaged in a decade-long cybercrime spree that deployed two of the most damaging pieces of financial malware ever used and resulted in tens of millions of dollars of losses to victims worldwide,” said Assistant Attorney General Benczkowski. “These two cases demonstrate our commitment to unmasking the perpetrators behind the world’s most egregious cyberattacks. The assistance of our international partners, in particular the National Crime Agency of the United Kingdom, was crucial to our efforts to identify Yakubets and his co-conspirators.”

“For over a decade, Maksim Yakubets and Igor Turashev led one of the most sophisticated transnational cybercrime syndicates in the world,” said U.S. Attorney Brady. “Deploying ‘Bugat’ malware, also known as ‘Cridex’ and ‘Dridex,’ these cybercriminals targeted individuals and companies in western Pennsylvania and across the globe in one of the most widespread malware campaigns we have ever encountered. International cybercriminals who target Pennsylvania citizens and companies are no different than any other criminal: they will be investigated, prosecuted and held accountable for their actions.”

“The Zeus scheme was one of the most outrageous cybercrimes in history,” said U.S. Attorney Kelly. “Our identification of Yakubets as the actor who used the moniker ‘aqua’ in that scheme, as alleged in the complaint unsealed today, is a prime example of how we will pursue cyber criminals to the ends of justice no matter how long it takes, by tracking their activity both online and off and working with our international partners to expose their crimes.”



"Today's announcement involved a long running investigation of a sophisticated organized cybercrime syndicate," said FBI Deputy Director Bowdich. "The charges highlight the persistence of the FBI and our partners to vigorously pursue those who desire to profit from innocent people through deception and theft. By calling out those who threaten American businesses and citizens, we expose criminals who hide behind devices and launch attacks that threaten our public safety and economic stability. The actions highlighted today, which represent a continuing trend of cyber-criminal activity emanating from Russian actors, were particularly damaging as they targeted U.S. entities across all sectors and walks of life. The FBI, with the assistance of private industry and our international and U.S. government partners, is sending a strong message that we will work together to investigate and hold all criminals accountable. Our memory is long and we will hold them accountable under the law, no matter where they attempt to hide."

"Combatting cybercrime remains a top national security priority for to the United States," said INL Principal Deputy Assistant Secretary of State Walsh. "The announcements today represent a coordinated interagency effort to bring Maksim Yakubets to justice and to address cybercrime globally."

"This is a landmark for the NCA, FBI and U.S. authorities and a day of reckoning for those who commit cybercrime," said NCA Director Jones. "Following years of online pursuit, I am pleased to see the real world identity of Yakubets and his associate Turashev revealed. Yakubets and his associates have allegedly been responsible for losses and attempted losses totaling hundreds of millions of dollars. This is not a victimless crime, those losses were once people's life savings, now emptied from their bank accounts. Today the process of bringing Yakubets and his criminal associates to justice begins. This is not the end of our investigation, and we will continue to work closely with international partners to present a united front against criminality that threatens our prosperity and security."

#### *Yakubets and Turashev Indicted in Relation to "Bugat" Malware*

A federal grand jury in Pittsburgh returned a 10-count indictment, which was unsealed today, against Yakubets and Turashev, charging them with conspiracy, computer hacking, wire fraud, and bank fraud, in connection with the distribution of "Bugat," a multifunction malware package designed to automate the theft of confidential personal and financial information, such as online banking credentials, from infected computers. Later versions of the malware were designed with the added function of assisting in the installation of ransomware.

According to the indictment, Bugat is a malware specifically crafted to defeat antivirus and other protective measures employed by victims. As the individuals behind Bugat improved the malware and added functionality, the name of the malware changed, at one point being called "Cridex," and later "Dridex," according to the indictment. Bugat malware was allegedly designed to automate the theft of confidential personal and financial information, such as online banking credentials, and facilitated the theft of confidential personal and financial information by a number of methods. For example, the indictment alleges that the Bugat malware allowed computer intruders to hijack a computer session and present a fake online banking webpage to trick a user into entering personal and financial information.

The indictment further alleges that Yakubets and Turashev used captured banking credentials to cause banks to make unauthorized electronic funds transfers from the victims' bank accounts, without the knowledge or consent of the account holders. They then allegedly used persons, known as "money mules," to receive stolen funds into their bank accounts, and then move the money to other accounts or withdraw the funds and transport the funds overseas as smuggled bulk cash. According to the indictment, they also used a powerful online tool known as a botnet in furtherance of the scheme.

Yakubets was the leader of the group of conspirators involved with the Bugat malware and botnet, according to the indictment. As the leader, he oversaw and managed the development, maintenance, distribution, and infection of Bugat as well as the financial theft and the use of money mules. Turashev allegedly handled a variety of functions for the Bugat conspiracy, including system administration, management of the internal control panel, and oversight of botnet operations.

According to the indictment, Yakubets and Turashev victimized multiple entities, including two banks, a school district, and four companies including a petroleum business, building materials supply company, vacuum and thin film deposition technology company and metal manufacturer in the Western District of Pennsylvania and a firearm manufacturer. The indictment alleges that these attacks resulted in the theft of millions of dollars, and occurred as recently as March 19, 2019.



*Yakubets Charged in Relation to "Zeus" Malware*

A criminal complaint was also unsealed in Lincoln today charging Yakubets with conspiracy to commit bank fraud in connection with the "Zeus" malware. Beginning in May 2009, Yakubets and multiple co-conspirators are alleged to have a long-running conspiracy to employ widespread computer intrusions, malicious software, and fraud to steal millions of dollars from numerous bank accounts in the United States and elsewhere. Yakubets and his co-conspirators allegedly infected thousands of business computers with malicious software that captured passwords, account numbers, and other information necessary to log into online banking accounts, and then used the captured information to steal money from victims' bank accounts. As with Bugat, the actors involved with the Zeus scheme were alleged to have employed the use of money mules and a botnet.

Yakubets and his co-conspirators are alleged to have victimized 21 specific municipalities, banks, companies, and non-profit organizations in California, Illinois, Iowa, Kentucky, Maine, Massachusetts, New Mexico, North Carolina, Ohio, Texas, and Washington, identified in the complaint, including multiple entities in Nebraska and a religious congregation. According to the complaint, the deployment of the Zeus malware resulted overall in the attempted theft of an estimated \$220 million USD, with actual losses of an estimated \$70 million USD from victims' bank accounts. According to the complaint, Yakubets' role in the Zeus scheme was to provide money mules and their associated banking credentials in order to facilitate the movement of money, which was withdrawn from victim accounts by fraudulent means.

An individual charged as John Doe #2, also known as "aqua," was indicted in District of Nebraska in case number 4:11-CR-3074. The indictment in that case charges that individual and others with conspiracy to participate in racketeering activity, conspiracy to commit computer fraud and identity theft, aggravated identity theft, and multiple counts of bank fraud related to the Zeus scheme. As alleged, the complaint unsealed today associates use of the moniker "aqua" in the Zeus scheme to Yakubets.

In case number 4:11-CR-3074, two of the co-conspirators of "aqua," Ukrainian nationals Yuriy Konovaleko and Yevhen Kulibaba, were extradited from the United Kingdom to the United States. Konovalenko and Kulibaba both pleaded guilty in 2015 to conspiracy to participate in racketeering activity and have completed prison sentences that were imposed. Konovalenko and Kulibaba were previously convicted in the United Kingdom, after an investigation conducted by the Metropolitan Police Service, for their role in laundering £3 million GBP on behalf of the group responsible for the Zeus malware.

*State Department \$5 million USD Reward*

The U.S. Department of State's Transnational Organized Crime (TOC) Rewards Program is offering a reward of up to \$5 million for information on Yakubets. Cyber threats are a top national security threat to the United States, and the Department of State's TOC Rewards Program is one of the many tools used by U.S. authorities to bring significant cybercriminals to justice. Congress established the TOC Rewards Program in 2013 to support law enforcement efforts to dismantle transnational criminal organizations and bring their leaders and members to justice. The U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs manages the program in coordination with other U.S. federal agencies.

In addition to NCA, the law enforcement actions taken related to these two prosecutions were assisted by the efforts of law enforcement counterparts from The Netherlands, Germany, Belarus, Ukraine, and the Russian Federation.

The FBI's Pittsburgh and Omaha Field Offices led the investigations of Yakubets and Turashev with assistance by the FBI's Major Cyber Crimes Unit and Global Operations and Targeting Unit. The prosecution in Pittsburgh is being handled by Assistant U.S. Attorney Shardul S. Desai of the Western District of Pennsylvania, and the prosecution in Lincoln is being handled by Senior Counsel William A. Hall, Jr., of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorney Steven A. Russell of the District of Nebraska. The Criminal Division's Office of International Affairs provided significant assistance throughout the criminal investigations. The Department's National Security Division also provided investigative assistance.

The details contained in the indictment, criminal complaint and related pleadings are merely accusations, and the defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

---

**Attachment(s):**

[Download Yakubets Turashev Indictment](#)

[Download Yakubets Complaint](#)

[Download Turashev Wanted Poster](#)

[Download Yakubets Wanted Poster](#)

**Topic(s):**

Cyber Crime

Financial Fraud

**Component(s):**

[Criminal Division](#)

[Criminal - Computer Crime and Intellectual Property Section](#)

[Criminal - Office of International Affairs](#)


[USAO - Nebraska](#)

[USAO - Pennsylvania, Western](#)

**Press Release Number:**

19-1346

*Updated November 19, 2020*

 An official website of the United States government  
[Here's how you know](#)



**Department of Justice**

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, October 16, 2019

**South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin**

**Dozens of Minor Victims Who Were Being Actively Abused by the Users of the Site Rescued**

Jong Woo Son, 23, a South Korean national, was indicted by a federal grand jury in the District of Columbia for his operation of Welcome To Video, the largest child sexual exploitation market by volume of content. The nine-count indictment was unsealed today along with a parallel civil forfeiture action. Son has also been charged and convicted in South Korea and is currently in custody serving his sentence in South Korea. An additional 337 site users residing in Alabama, Arkansas, California, Connecticut, Florida, Georgia, Kansas, Louisiana, Maryland, Massachusetts, Nebraska, New Jersey, New York, North Carolina, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Texas, Utah, Virginia, Washington State and Washington, D.C. as well as the United Kingdom, South Korea, Germany, Saudi Arabia, the United Arab Emirates, the Czech Republic, Canada, Ireland, Spain, Brazil and Australia have been arrested and charged.

Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney Jessie K. Liu for the District of Columbia, Chief Don Fort of IRS Criminal Investigation (IRS-CI) and Acting Executive Associate Director Alysa Erichs of U.S. Immigration and Customs Enforcement (ICE)'s Homeland Security Investigations (HSI), made the announcement.

"Darknet sites that profit from the sexual exploitation of children are among the most vile and reprehensible forms of criminal behavior," said Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division. "This Administration will not allow child predators to use lawless online spaces as a shield. Today's announcement demonstrates that the Department of Justice remains firmly committed to working closely with our partners in South Korea and around the world to rescue child victims and bring to justice the perpetrators of these abhorrent crimes."

"Children around the world are safer because of the actions taken by U.S. and foreign law enforcement to prosecute this case and recover funds for victims," said U.S. Attorney Jessie K. Liu. "We will continue to pursue such criminals on and off the darknet in the United States and abroad, to ensure they receive the punishment their terrible crimes deserve."

"Through the sophisticated tracing of bitcoin transactions, IRS-CI special agents were able to determine the location of the Darknet server, identify the administrator of the website and ultimately track down the website server's physical location in South Korea," said IRS-CI Chief Don Fort. "This large-scale criminal enterprise that endangered the safety of children around the world is no more. Regardless of the illicit scheme, and whether the proceeds are virtual or tangible, we will continue to work with our federal and international partners to track down these disgusting organizations and bring them to justice."

"Children are our most vulnerable population, and crimes such as these are unthinkable," said HSI Acting Executive Associate Director Alysa Erichs. "Sadly, advances in technology have enabled child predators to hide behind the dark

web and cryptocurrency to further their criminal activity. However, today's indictment sends a strong message to criminals that no matter how sophisticated the technology or how widespread the network, child exploitation will not be tolerated in the United States. Our entire justice system will stop at nothing to prevent these heinous crimes, safeguard our children, and bring justice to all."

According to the indictment, on March 5, 2018, agents from the IRS-CI, HSI, National Crime Agency in the United Kingdom, and Korean National Police in South Korea arrested Son and seized the server that he used to operate a Darknet market that exclusively advertised child sexual exploitation videos available for download by members of the site. The operation resulted in the seizure of approximately eight terabytes of child sexual exploitation videos, which is one of the largest seizures of its kind. The images, which are currently being analyzed by the National Center for Missing and Exploited Children (NCMEC), contained over 250,000 unique videos, and 45 percent of the videos currently analyzed contain new images that have not been previously known to exist.

Welcome To Video offered these videos for sale using the cryptocurrency bitcoin. Typically, sites of this kind give users a forum to trade in these depictions. This Darknet website is among the first of its kind to monetize child exploitation videos using bitcoin. In fact, the site itself boasted over one million downloads of child exploitation videos by users. Each user received a unique bitcoin address when the user created an account on the website. An analysis of the server revealed that the website had more than one million bitcoin addresses, signifying that the website had capacity for at least one million users.

The agencies have shared data from the seized server with law enforcement around the world to assist in identifying and prosecuting customers of the site. This has resulted in leads sent to 38 countries and yielded arrests of 337 subjects around the world. The operation has resulted in searches of residences and businesses of approximately 92 individuals in the United States. Notably, the operation is responsible for the rescue of at least 23 minor victims residing in the United States, Spain and the United Kingdom, who were being actively abused by the users of the site.

In the Washington, D.C.-metropolitan area, the operation has led to the execution of five search warrants and eight arrests of individuals who both conspired with the administrator of the site and were themselves, users of the website. Two users of the Darknet market committed suicide subsequent to the execution of search warrants.

Amongst the sites users charged are:

- Charles Wunderlich, 34, of Hot Springs, California, was charged in the District of Columbia with conspiracy to distribute child pornography;
- Brian James LaPrath, 34, of San Diego, California, was arrested in the District of Columbia, for international money laundering; and was sentenced to serve 18 months in prison followed by three years of supervised release;
- Ernest Wagner, 70, of Federal Way, Washington, was arrested and charged in the District of Columbia with conspiracy to distribute child pornography;
- Vincent Galarzo, 28, of Glendale, New York, was arrested and charged in the District of Columbia with conspiracy to distribute child pornography;
- Michael Ezeagbor, 22, of Pflugerville, Texas, was arrested and charged in the District of Columbia with conspiracy to distribute child pornography;
- Nicholas Stengel, 45, of Washington, D.C., pleaded guilty to receipt of child pornography and money laundering and was sentenced to serve 15 years in prison followed by a lifetime of supervised release;
- Eryk Mark Chamberlin, 25, of Worcester, Massachusetts, pleaded guilty to possession of child pornography and is pending sentencing;
- Jairo Flores, 30, of Cambridge, Massachusetts, pleaded guilty in the District of Massachusetts to receipt and possession of child pornography and was sentenced to serve five years in prison followed by five years of

supervised release;

- Billy Penaloza, 29, of Dorchester, Massachusetts, pleaded guilty in the District of Massachusetts to possession and receipt of child pornography. His sentencing is scheduled for Oct. 22, 2019;
- Michael Armstrong, 35, of Randolph, Massachusetts, pleaded guilty in the District of Massachusetts, to receipt and possession of child pornography. He was sentenced to serve five years in prison followed by five years of supervised release. Restitution will be determined at a future date;
- Al Ramadhanu Soedomo, 28, of Lynn, Massachusetts, pleaded guilty to possession of child pornography and was sentenced in the District of Massachusetts (Boston), to serve 12 months and one day followed by five years of supervised release;
- Phillip Sungmin Hong, 24, of Sharon, Massachusetts, pleaded guilty in the District of Massachusetts (Boston), to receipt and possession of child pornography and is pending sentencing;
- Eliseo Arteaga Jr., 28, of Mesquite, Texas, pleaded guilty in the Northern District of Texas to possession of prepubescent child pornography. He is pending sentencing;
- Richard Nikolai Gratkowski, 40, of San Antonio, Texas, a former HSI special agent, was arrested in the Western District of Texas. Gratkowski pleaded guilty to the indictment charging one count of receipt of child pornography and one count of access with intent to view child pornography. Gratkowski was sentenced to serve 70 months in prison followed by 10 years of supervised release, and ordered to pay \$35,000 in restitution to seven victims and a \$10,000 assessment;
- Paul Casey Whipple, 35, of Hondo, Texas, a U.S. Border Patrol Agent, was arrested in the Western District of Texas, on charges of sexual exploitation of children/minors, production, distribution, and possession of child pornography. Whipple remains in custody awaiting trial in San Antonio;
- Michael Lawson, 36, of Midland, Georgia, was arrested in the Middle District of Georgia on charges of attempted sexual exploitation of children and possession of child pornography. He was sentenced to serve 121 months in prison followed by 10 years of supervised release following his plea to a superseding information charging him with one count of receipt of child pornography;
- Kevin Christopher Eagan, 39, of Brookhaven, Georgia, pleaded guilty to possession of child pornography in the Northern District of Georgia;
- Casey Santioius Head, 37, of Griffin, Georgia, was indicted in the Northern District of Georgia for distribution, receipt, and possession of child pornography;
- Andrew C. Chu, 28, of Garwood, New Jersey, was arrested and charged with receipt of child pornography. Those charges remain pending;
- Nader Hamdi Ahmed, 29 of Jersey City, New Jersey, was arrested in the District of New Jersey, for sexual exploitation or other abuse of children. Ahmed pleaded guilty to an information charging him with one count of distribution of child pornography. He is scheduled to be sentenced Oct. 1, 2019;
- Jeffrey Lee Harris, 32, of Pickens, South Carolina, pleaded guilty in the District of South Carolina for producing, distributing, and possessing child pornography;
- Laine Ormand Clark Jr., 27, of Conway, South Carolina, was arrested and charged in U.S. District Court in South Carolina Division for sexual possession of child pornography;

- Jack R. Dove III, 38, of Lakeland, Florida, was arrested in the Middle District of Florida for knowingly receiving and possessing visual depictions of minors engaged in sexually explicit conduct;
- Michael Matthew White, 39, of Miami Beach, Florida, was arrested in the Southern District of Florida for coercion and enticement;
- Nikolas Bennion Bradshaw, 24, of Bountiful, Utah, was arrested in the State of Utah, and charged with five counts of sexual exploitation of a minor, and was sentenced to time served with 91 days in jail followed by probation;
- Michael Don Gibbs, 37, of Holladay, Utah, was charged in the District of Utah with receipt of child pornography and possession of child pornography;
- Ammar Atef H. Alahdali, 22, of Arlington, Virginia, pleaded guilty in the Eastern District of Virginia to receipt of child pornography and was sentenced to serve five years in prison and ordered to pay \$3,000 in restitution;
- Mark Lindsay Rohrer, 38, of West Hartford, Connecticut, pleaded guilty in the District of Connecticut to receipt of child pornography and was sentenced to serve 60 months in prison followed by five years of supervised release;
- Eugene Edward Jung, 47, of San Francisco, California, was indicted in the Northern District of California on possession of child pornography and receipt of child pornography;
- James Daosaeng, 25, of Springdale, Arkansas, pleaded guilty to possession of child pornography and was sentenced in the Western District of Arkansas (Fayetteville) to serve 97 months in prison followed by 20 years of supervised release;
- Alex Daniel Paxton, 30, of Columbus, Ohio, was arrested and indicted in Franklin County Ohio Court of Common Pleas for pandering sexually oriented matter involving a minor;
- Don Edward Pannell, 32, of Harvey, Louisiana, pleaded guilty in the Eastern District of Louisiana for receipt of child pornography. He is pending sentencing;
- Ryan Thomas Carver, 29, of Huntsville, Alabama, was arrested and charged under Alabama State Law. He was charged federally in the Northern District of Alabama with possession of child pornography. His case is pending in Huntsville, Alabama;
- Alexander Buckley, 28, of the United Kingdom, pleaded guilty to 10 offences in the UK of possession and distribution of indecent images of children, possession of extreme and prohibited images and possession of a class A drug. He was sentenced to serve 40 months in prison for the distribution of indecent images and possession of class A drugs. Buckley is also subject to an indefinite Sexual Harm Prevention Order;
- Kyle Fox, 26, of the United Kingdom, pleaded guilty to 22 counts including rape, sexual assault, and sharing indecent images, and was sentenced to serve 22 years in prison; and
- Mohammed Almaker, 26, of Fort Collins, Colorado, was arrested in the Kingdom of Saudi Arabia (KSA), charged with KSA Law involving the endangerment of children. He is awaiting judicial proceedings in furtherance of criminal charges.

A forfeiture complaint was also unsealed today. The complaint alleges that law enforcement was able to trace payments of bitcoin to the Darknet site by following the flow of funds on the blockchain. The virtual currency accounts identified in the complaint were allegedly used by 24 individuals in five countries to fund the website and promote the exploitation of children. The forfeiture complaint seeks to recover these funds and, ultimately through the restoration process, return the illicit funds to victims of the crime.

The charges in the indictment are merely allegations, and all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The international investigations were led by the IRS-CI, HSI and the NCA. The Korean National Police of the Republic of Korea, the National Crime Agency of the United Kingdom and the German Federal Criminal Police (the Bundeskriminalamt), provided assistance and coordinated with their parallel investigations. The Department of Justice's Office of International Affairs of the Criminal Division provided significant assistance.

The cases are being handled by Assistant U.S. Attorneys Zia M. Faruqui, Lindsay Suttenger, and Youli Lee, Paralegal Specialists Brian Rickers and Diane Brashears, Legal Assistant Jessica McCormick, and Records Examiner Chad Byron of the U.S. Attorney's Office for the District of Columbia and Trial Attorney C. Alden Pelker of the Criminal Division's Computer Crime and Intellectual Property Section. Additional assistance has been provided by Deputy Chief Keith Becker and Trial Attorney James E. Burke IV of the Criminal Division's Child Exploitation and Obscenity Section, and former U.S. Attorney's Office Paralegal Specialists Toni Anne Donato and Ty Eaton.

---

**Attachment(s):**

[Download Son Indictment](#)

[Download Graphic of Seizure Page](#)

[Download Screen Shot of Webpage](#)

[Download Complaint for Forfeiture](#)

**Topic(s):**

Cyber Crime

**Component(s):**

[Criminal Division](#)

[Criminal - Child Exploitation and Obscenity Section](#)

[Criminal - Computer Crime and Intellectual Property Section](#)

[Criminal - Office of International Affairs](#)


[USAO - District of Columbia](#)

**Press Release Number:**

19-1,104

*Updated December 7, 2020*



 An official website of the United States government  
[Here's how you know](#)



## Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, September 10, 2019

# **281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes**

## **74 Alleged Fraudsters Arrested in the United States**

Federal authorities announced today a significant coordinated effort to disrupt Business Email Compromise (BEC) schemes that are designed to intercept and hijack wire transfers from businesses and individuals, including many senior citizens. Operation reWired, a coordinated law enforcement effort by the U.S. Department of Justice, U.S. Department of Homeland Security, U.S. Department of the Treasury, U.S. Postal Inspection Service, and the U.S. Department of State, was conducted over a four-month period, resulting in 281 arrests in the United States and overseas, including 167 in Nigeria, 18 in Turkey and 15 in Ghana. Arrests were also made in France, Italy, Japan, Kenya, Malaysia, and the United Kingdom (UK). The operation also resulted in the seizure of nearly \$3.7 million.

BEC, also known as “cyber-enabled financial fraud,” is a sophisticated scam often targeting employees with access to company finances and businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The same criminal organizations that perpetrate BEC also exploit individual victims, often real estate purchasers, the elderly, and others, by convincing them to make wire transfers to bank accounts controlled by the criminals. This is often accomplished by impersonating a key employee or business partner after obtaining access to that person’s email account or sometimes done through romance and lottery scams. BEC scams may involve fraudulent requests for checks rather than wire transfers; they may target sensitive information such as personally identifiable information (PII) or employee tax records instead of, or in addition to, money; and they may not involve an actual “compromise” of an email account or computer network. Foreign citizens perpetrate many BEC scams. Those individuals are often members of transnational criminal organizations, which originated in Nigeria but have spread throughout the world.

“The Department of Justice has increased efforts in taking aggressive enforcement action against fraudsters who are targeting American citizens and their businesses in business email compromise schemes and other cyber-enabled financial crimes,” said Deputy Attorney General Jeffrey Rosen. “In this latest four-month operation, we have arrested 74 people in the United States and 207 others have been arrested overseas for alleged financial fraud. The coordinated efforts with our domestic and international law enforcement partners around the world has made these most recent actions more successful. I want to thank the FBI, more than two dozen U.S. Attorney’s Offices, U.S. Secret Service, U.S. Postal Inspection Service, Homeland Security Investigations, IRS Criminal Investigation, U.S. Department of State’s Diplomatic Security Service, our partners in Nigeria, Ghana, Turkey, France, Italy, Japan, Kenya, Malaysia, and the UK, and our state and local law enforcement partners for all of their hard work to combat these fraud schemes and protect the hard-earned assets of our citizens. Anyone who engages in deceptive practices like this should know they will not go undetected and will be held accountable.”

“The FBI is working every day to disrupt and dismantle the criminal enterprises that target our businesses and our citizens,” said FBI Director Christopher A. Wray. “Cooperation is the backbone to effective law enforcement; without it, we aren’t as strong or as agile as we need to be. Through Operation reWired, we’re sending a clear message to the

criminals who orchestrate these BEC schemes: We'll keep coming after you, no matter where you are. And to the public, we'll keep doing whatever we can to protect you. Reporting incidents of BEC and other internet-enabled crimes to the IC3 brings us one step closer to the perpetrators."

"The Secret Service has taken a multi-layered approach to combating Business Email Compromise schemes through our Global Investigative Operations Center (GIOC)," said U.S. Secret Service Director James M. Murray. "Domestically, the GIOC assists Secret Service Field Offices and other law enforcement partners with analysis and investigative tactics to enhance the impact of local BEC investigations. Internationally, the GIOC targets and identifies transnational organized crime networks that perpetrate these cyber-enabled financial fraud schemes. Through this approach, the Secret Service continues to strive to protect the citizens of the United States and our financial infrastructure from these complex crimes."

"Homeland Security Investigations (HSI), together with its law enforcement partners, has proven once again, that cyber-enabled financial fraud will not be tolerated in the United States," said Acting Director Matthew T. Albence of U.S. Immigration and Customs Enforcement (ICE). "Operation reWired sends a clear message to criminals, that no matter how or where crimes are committed, we will do everything within our means to dismantle criminal enterprises that seek to manipulate U.S. institutions and taxpayers."

"The consequences of this type of fraud scheme are far reaching, affecting not only people in the United States, but also across the world," said Chief Postal Inspector Gary Barksdale. "This investigation is just another example of how effective law enforcement agencies can be when they join forces. By working together, we can keep our communities and our vulnerable populations safe from financial exploitation. The U.S. Postal Inspection Service is proud to be at the forefront of the fight against fraud and Postal Inspectors will continue to adapt to the ever changing landscape to stop the scammers and protect our customers."

"In unraveling this complex, nationwide identity theft and tax fraud scheme, we discovered that the conspirators stole more than 250,000 identities and filed more than 10,000 fraudulent tax returns, attempting to receive more than \$91 million in refunds," said Chief Don Fort of IRS Criminal Investigation. "We will continue to work with our international, federal and state partners to pursue all those responsible for perpetrating this fraud, preying on innocent victims and attempting to cheat the U.S. out of millions of dollars."

"The investigation of these crimes crossed international borders," said Director Todd J. Brown of the U.S. Department of State's Diplomatic Security Service (DSS). "Today's charges are another successful example of our commitment to working together with both foreign colleagues abroad as well as local, state and federal law enforcement partners here at home in the pursuit of those who commit cyber-related financial crimes."

A number of cases involved international criminal organizations that defrauded small to large sized businesses, while others involved individual victims who transferred high dollar funds or sensitive records in the course of business. The devastating effects these cases have on victims and victim companies affect not only the individual business but also the global economy. According to the Internet Crime Complaint Center (IC3), nearly \$1.3 billion in loss was reported in 2018 from BEC and its variant, Email Account Compromise (EAC), nearly twice as much as was reported the prior year. BEC and EAC are prevalent scams and the Justice Department along with our partners will continue to aggressively pursue and prosecute the perpetrators, including money mules, regardless of where they are located.

Money mules may be witting or unwitting accomplices who receive ill-gotten funds from the victims and then transfer the funds as directed by the fraudsters. The money is wired or sent by check to the money mule who then deposits it in his or her own bank account. Usually the mules keep a fraction for "their trouble" and then wire the money as directed by the fraudster. The fraudsters enlist and manipulate the money mules through romance scams or "work-at-home" scams, though some money mules are knowing co-conspirators who launder the ill-gotten gains for profit.

BEC scams are related to, and often conducted together with, other forms of fraud such as:

- "Romance scams," where victims are lulled into believing they are in a legitimate relationship, and are tricked into sending or laundering money under the guise of assisting the paramour with an international business transaction, a U.S. visit, or some other cover story;

- “Employment opportunities scams,” where victims are convinced to provide their PII to apply for work-from-home jobs, and, once “hired” and “overpaid” by a bad check, to wire the overpayment to the “employer’s” bank before the check bounces;
- “Fraudulent online vehicle sales scams,” where victims are convinced they are purchasing a nonexistent vehicle and must pay for it by sending the codes of prepaid gift cards in the amount of the agreed upon sale price to the “seller;”
- “Rental scams,” where a scammer agrees to rent a property, sends a bad check in excess of the agreed upon deposit, and requests the overpayment be returned via wire before the check bounces; and
- “Lottery scams,” where victims are convinced they won an international lottery but must pay fees or taxes before receiving the payout.

Starting in May 2019, this coordinated enforcement action targeted hundreds of BEC scammers. Law enforcement agents executed over 214 domestic actions including arrests, money mule warning letters, and asset seizures and repatriations totaling nearly \$3.7 million. Local and state law enforcement partners on FBI task forces across the country, with the assistance of multiple District Attorney’s Offices, also arrested alleged money mules for their role in defrauding victims.

Among those arrested on federal charges in BEC schemes include:

- Following an investigation led by the FBI’s Chicago Division, Brittney Stokes, 27, of Country Club Hills, Illinois, and Kenneth Ninalowo, 40, of Chicago, Illinois, were charged in the Northern District of Illinois with laundering over \$1.5 million from proceeds of BEC scams. According to the indictment, a community college and an energy company were defrauded into sending approximately \$5 million to fraudulent bank accounts controlled by the scammers. Banks were able to freeze approximately \$3.6 million of the \$5 million defrauded in the two schemes. Law enforcement officials seized a 2019 Range Rover Velar S from Stokes and approximately \$175,909 from Stokes and Ninalowo.
- As a result of a joint investigation by the FBI, HSI, and DSS, Opeyemi Adeoso, 44, of Dallas, Texas, and Benjamin Ifebajo, 45, of Richardson, Texas, were arrested and charged in the Northern District of Texas with bank fraud, wire fraud, money laundering, and conspiracy. Adeoso and Ifebajo are alleged to have received and laundered at least \$3.4 million. In furtherance of their scheme, they are alleged to have assumed 12 fictitious identities and defrauded 37 victims from across the United States.
- As part of a larger investigation by the FBI and the USSS in Miami, Yamel Guevara Tamayo, 36, of Miami, Florida, and Yumeydi Govantes, 39, of Miami, Florida, were charged in the Southern District of Florida with laundering more than \$950,000 of proceeds of BEC scams. The two individuals were also responsible for recruiting approximately 18 other individuals to serve as money mules, who laundered proceeds of BEC scams for an international money laundering network. The victims of the BEC scams included title companies, corporations, and individuals. The individuals were indicted June 18, 2019 and arrested June 20, 2019. The change of plea for both individuals is scheduled for Sept. 16.
- In an investigation by FBI Atlanta, two individuals were charged in the Northern District of Georgia for their involvement in a Nigeria-based BEC scheme that began with a \$3.5 million transfer of funds fraudulently misdirected from a Georgia-based health care provider to accounts across the United States. Two Nigerian nationals, Emmanuel Igomu, 35, of Atlanta, Georgia, and Jude Balogun, 29, of San Francisco, California, have been arrested on charges of aiding and abetting wire fraud for their part in receiving and transmitting monies derived from the BEC.
- Following an investigation by the FBI, Cyril Ashu, 34, of Austell, Georgia; Ifeanyi Eke, 32, of Sandy Springs, Georgia; Joshua Ikejimba, 24, of Houston, Texas; and Chinedu Ironuah, 32, of Houston, Texas, were charged in the Southern District of New York with one count of conspiracy to commit wire fraud and one count of wire fraud

for their involvement in a Nigeria-based BEC scheme that impacted hundreds of victims in the United States, with losses in excess of \$10 million.

An indictment is merely an allegation and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The cases were investigated by the FBI, U.S. Secret Service, U.S. Postal Inspection Service, ICE's Homeland Security Investigations (HSI), IRS Criminal Investigation and U.S. Department of State's Diplomatic Security Service. U.S. Attorney's Offices in the Districts of Arizona; Central, Eastern and Southern California; Colorado; Delaware; Southern Florida; Northern Georgia; Northern Illinois; Kansas; Eastern Louisiana; Massachusetts; Nebraska; Nevada; Southern New York; Middle North Carolina; Northern Ohio; Oregon; Northern, Western and Southern Texas; Western Tennessee; Eastern Virginia; Eastern Washington, and elsewhere have ongoing investigations some of which have resulted in arrests in Nigeria. The Justice Department's Computer Crime and Intellectual Property Section, Money Laundering and Asset Recovery Section, and Office of International Affairs of the Criminal Division provided assistance. District Attorney's Offices of Harris County, Texas; Fort Bend County, Texas; and Washington County, Arkansas are handling state prosecutions. Additionally, private sector partners and the Nigerian Economic and Financial Crimes Commission, Ghana Police Service (GPS) and Economic and Organized Crime Office (EOCO), Turkish National Police (TNP) Cyber Department, Direction Centrale de la Police aux Frontieres (PAF) of France, Squadra Mobile Di Caserta and Italian National Police, National Police Agency of Japan, Tokyo Metropolitan Police Department (TPMD), Royal Malaysian Police, Directorate of Criminal Investigations (DCI) of Kenya and the National Crime Agency (NCA), North Wales Police, Metropolitan Police Service and Hertfordshire Constabulary of the UK provided significant assistance.

This operation serves as a model for international cooperation against specific threats that endanger the financial well-being of each member country's residents. Deputy Attorney General Rosen expressed gratitude for the outstanding efforts of the participating countries, including law enforcement actions that were coordinated and executed by the Economic and Financial Crimes Commission (EFCC) in Nigeria to curb business email compromise schemes that defraud businesses and individuals alike.

The Justice Department's efforts to confront the growing threat of cyber-enabled financial fraud led to the formation of the BEC Counteraction Group (BCG), which assists U.S. Attorney's Offices and the Department with the coordination of BEC cases and the centralization of related expertise. The BCG facilitates communication and coordination between federal prosecutors, serves as a bridge between federal prosecutors and federal agents, centralizes and manages institutional knowledge and training, and participates in efforts to educate the public about protecting themselves and their organizations from BEC scams.

The BCG draws upon the expertise of the following sections within the Department's Criminal Division: the Computer Crime and Intellectual Property Section, which regularly investigates and prosecutes cases involving computer crimes, including network intrusions; the Fraud Section, which manages complex litigation involving sophisticated fraud schemes; the Money Laundering and Asset Recovery Section, which brings experience in seizing assets obtained through criminal activity; the Office of International Affairs, which plays a central role in securing international evidence and extradition; and the Organized Crime and Gang Section, which contributes strategic guidance in prosecuting complex transnational criminal cases.

Operation reWired was funded and coordinated by the FBI and the Justice Department's International Organized Crime Intelligence and Operations Center (IOC-2) and follows "Operation Wire Wire," the first coordinated enforcement action targeting hundreds of BEC scammers. That effort, announced in June 2018, resulted in the arrest of 74 individuals, the seizure of nearly \$2.4 million, and the disruption and recovery of approximately \$14 million in fraudulent wire transfers.

Victims are encouraged to file a complaint online with the IC3 at [bec.ic3.gov](https://www.ic3.gov). The IC3 staff reviews complaints, looking for patterns or other indicators of significant criminal activity, and refers investigative packages of complaints to the appropriate law enforcement authorities in a particular city or region. The FBI provides a variety of resources relating to BEC through the IC3, which can be reached at [www.ic3.gov](https://www.ic3.gov).

For more information on BEC scams, visit: <https://www.ic3.gov/media/2019/190910.aspx>.

---

**Topic(s):**

Consumer Protection

Cyber Crime

Financial Fraud


**Component(s):**

Office of the Deputy Attorney General

**Press Release Number:**

19-955

*Updated September 23, 2019*

 An official website of the United States government  
[Here's how you know](#)



**Department of Justice**

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, September 6, 2018

## **North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions**

### **North Korean Hacking Team Responsible for Global WannaCry 2.0 Ransomware, Destructive Cyberattack on Sony Pictures, Central Bank Cybertheft in Bangladesh, and Other Malicious Activities**

A criminal complaint was unsealed today charging Park Jin Hyok (박진혁; a/k/a Jin Hyok Park and Pak Jin Hek), a North Korean citizen, for his involvement in a conspiracy to conduct multiple destructive cyberattacks around the world resulting in damage to massive amounts of computer hardware, and the extensive loss of data, money and other resources (the "Conspiracy").

The complaint alleges that Park was a member of a government-sponsored hacking team known to the private sector as the "Lazarus Group," and worked for a North Korean government front company, Chosun Expo Joint Venture (a/k/a Korea Expo Joint Venture or "KEJV"), to support the DPRK government's malicious cyber actions.

The Conspiracy's malicious activities include the creation of the malware used in the 2017 WannaCry 2.0 global ransomware attack; the 2016 theft of \$81 million from Bangladesh Bank; the 2014 attack on Sony Pictures Entertainment (SPE); and numerous other attacks or intrusions on the entertainment, financial services, defense, technology, and virtual currency industries, academia, and electric utilities.

The charges were announced by Attorney General Jeff Sessions, FBI Director Christopher A. Wray, Assistant Attorney General for National Security John C. Demers, First Assistant United States Attorney for the Central District of California Tracy Wilkison and Assistant Director in Charge Paul D. Delacourt of the FBI's Los Angeles Field Office.

In addition to these criminal charges, Treasury Secretary Steven Mnuchin announced today that the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated Park and KEJV under Executive Order 13722 based on the malicious cyber and cyber-enabled activity outlined in the criminal complaint.

"Today's announcement demonstrates the FBI's unceasing commitment to unmasking and stopping the malicious actors and countries behind the world's cyberattacks," said FBI Director Christopher Wray. "We stand with our partners to name the North Korean government as the force behind this destructive global cyber campaign. This group's actions are particularly egregious as they targeted public and private industries worldwide – stealing millions of dollars, threatening to suppress free speech, and crippling hospital systems. We'll continue to identify and illuminate those responsible for malicious cyberattacks and intrusions, no matter who or where they are."

"The scale and scope of the cyber-crimes alleged by the Complaint is staggering and offensive to all who respect the rule of law and the cyber norms accepted by responsible nations," said Assistant Attorney General Demers. "The Complaint alleges that the North Korean government, through a state-sponsored group, robbed a central bank and citizens of other nations, retaliated against free speech in order to chill it half a world away, and created disruptive malware that indiscriminately affected victims in more than 150 other countries, causing hundreds of millions, if not billions, of dollars' worth of damage. The investigation, prosecution, and other disruption of malicious state-sponsored



cyber activity remains among the highest priorities of the National Security Division and I thank the FBI agents, DOJ prosecutors, and international partners who have put years of effort into this investigation.”

“The complaint charges members of this North Korean-based conspiracy with being responsible for cyberattacks that caused unprecedented economic damage and disruption to businesses in the United States and around the globe,” said First Assistant United States Attorney Tracy Wilkison. “The scope of this scheme was exposed through the diligent efforts of FBI agents and federal prosecutors who were able to unmask these sophisticated crimes through sophisticated means. They traced the attacks back to the source and mapped their commonalities, including similarities among the various programs used to infect networks across the globe. These charges send a message that we will track down malicious actors no matter how or where they hide. We will continue to pursue justice for those responsible for the huge monetary losses and attempting to compromise the national security of the United States.”

“We will not allow North Korea to undermine global cybersecurity to advance its interests and generate illicit revenues in violation of our sanctions,” said Treasury Secretary Steven Mnuchin. “The United States is committed to holding the regime accountable for its cyber-attacks and other crimes and destabilizing activities.”

Park is charged with one count of conspiracy to commit computer fraud and abuse, which carries a maximum sentence of five years in prison, and one count of conspiracy to commit wire fraud, which carries a maximum sentence of 20 years in prison.

### ***About the Defendant Park and Chosun Expo Joint Venture***

According to the allegations contained in the criminal complaint, which was filed on June 8, 2018 in Los Angeles federal court, and posted today: Park Jin Hyok, was a computer programmer who worked for over a decade for Chosun Expo Joint Venture (a/k/a Korea Expo Joint Venture or “KEJV”). Chosun Expo Joint Venture had offices in China and the DPRK, and is affiliated with Lab 110, a component of DPRK military intelligence. In addition to the programming done by Park and his group for paying clients around the world, the Conspiracy also engaged in malicious cyber activities. Security researchers that have independently investigated these activities referred to this hacking team as the “Lazarus Group.” The Conspiracy’s methods included spear-phishing campaigns, destructive malware attacks, exfiltration of data, theft of funds from bank accounts, ransomware extortion, and propagating “worm” viruses to create botnets.

### ***The Conspiracy’s Cyber Attacks, Heists, and Intrusions***

The complaint describes a broad array of the Conspiracy’s alleged malicious cyber activities, both successful and unsuccessful, and in the United States and abroad, with a particular focus on four specific examples.

#### ***Targeting the Entertainment Industry***

In November 2014, the conspirators launched a destructive attack on Sony Pictures Entertainment (SPE) in retaliation for the movie “The Interview,” a farcical comedy that depicted the assassination of the DPRK’s leader. The conspirators gained access to SPE’s network by sending malware to SPE employees, and then stole confidential data, threatened SPE executives and employees, and damaged thousands of computers. Around the same time, the group sent spear-phishing messages to other victims in the entertainment industry, including a movie theater chain and a U.K. company that was producing a fictional series involving a British nuclear scientist taken prisoner in DPRK.

#### ***Targeting Financial Services***

In February 2016, the Conspiracy stole \$81 million from Bangladesh Bank. As part of the cyber-heist, the Conspiracy accessed the bank’s computer terminals that interfaced with the Society for Worldwide Interbank Financial Telecommunication (SWIFT) communication system after compromising the bank’s computer network with spear-phishing emails, then sent fraudulently authenticated SWIFT messages directing the Federal Reserve Bank of NY to transfer funds from Bangladesh to accounts in other Asian countries. The Conspiracy attempted to and did gain access to several other banks in various countries from 2015 through 2018 using similar methods and “watering hole attacks,” attempting the theft of at least \$1 billion through such operations.

#### ***Targeting of U.S. Defense Contractors***



In 2016 and 2017, the Conspiracy targeted a number of U.S. defense contractors, including Lockheed Martin, with spear-phishing emails. These malicious emails used some of the same aliases and accounts seen in the SPE attack, at times accessed from North Korean IP addresses, and contained malware with the same distinct data table found in the malware used against SPE and certain banks, the complaint alleges. The spear-phishing emails sent to the defense contractors were often sent from email accounts that purported to be from recruiters at competing defense contractors, and some of the malicious messages made reference to the Terminal High Altitude Area Defense (THAAD) missile defense system deployed in South Korea. The attempts to infiltrate the computer systems of Lockheed Martin, the prime contractor for the THAAD missile system, were not successful.

### ***Creation of Wannacry 2.0***

In May 2017, a ransomware attack known as WannaCry 2.0 infected hundreds of thousands of computers around the world, causing extensive damage, including significantly impacting the United Kingdom's National Health Service. The Conspiracy is connected to the development of WannaCry 2.0, as well as two prior versions of the ransomware, through similarities in form and function to other malware developed by the hackers, and by spreading versions of the ransomware through the same infrastructure used in other cyber-attacks.

Park and his co-conspirators were linked to these attacks, intrusions, and other malicious cyber-enabled activities through a thorough investigation that identified and traced: email and social media accounts that connect to each other and were used to send spear-phishing messages; aliases, malware "collector accounts" used to store stolen credentials; common malware code libraries; proxy services used to mask locations; and North Korean, Chinese, and other IP addresses. Some of this malicious infrastructure was used across multiple instances of the malicious activities described herein. Taken together, these connections and signatures—revealed in charts attached to the criminal complaint—show that the attacks and intrusions were perpetrated by the same actors.

### ***Accompanying Mitigation Efforts***

Throughout the course of the investigation, the FBI and the Department provided specific information to victims about how they had been targeted or compromised, as well as information about the tactics and techniques used by the conspiracy with the goals of remediating any intrusion and preventing future intrusions. That direct sharing of information took place in the United States and in foreign countries, often with the assistance of foreign law enforcement partners. The FBI also has collaborated with certain private cybersecurity companies by sharing and analyzing information about the intrusion patterns used by the members of the conspiracy.

In connection with the unsealing of the criminal complaint, the FBI and prosecutors provided cybersecurity providers and other private sector partners detailed information on accounts used by the Conspiracy in order to assist these partners in their own independent investigative activities and disruption efforts.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendant will be determined by the assigned judge.

This case is being prosecuted by Assistant United States Attorneys Stephanie S. Christensen, Anthony J. Lewis, and Anil J. Antony of the United States Attorney's Office for the Central District of California, and DOJ Trial Attorneys David Aaron and Scott Claffee of the National Security Division's Counterintelligence and Export Control Section. The Criminal Division's Office of International Affairs provided assistance throughout this investigation, as did many of the FBI's Legal Attachés, and foreign authorities around the world.

The charges contained in the criminal complaint are merely accusations and the defendant is presumed innocent unless and until proven guilty.

For the U.S. Department of Treasury's press release announcing corresponding sanctions please visit [www.treasury.gov](http://www.treasury.gov).

---

### **Attachment(s):**

Download 2018 09 06 Park Complaint Unsealed

### **Topic(s):**

Counterintelligence and Export Control  
National Security


**Component(s):**

National Security Division (NSD)  
USAO - California, Central

**Press Release Number:**

18-1452

*Updated September 6, 2018*

 An official website of the United States government  
[Here's how you know](#)



**Department of Justice**

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, July 20, 2017

## **AlphaBay, the Largest Online 'Dark Market,' Shut Down**

### **'Dark Net' Site Was Major Source of Fentanyl and Heroin, Linked to Overdose Deaths, and Used By Hundreds of Thousands of People to Buy and Sell Illegal Goods and Services Anonymously over the Internet**

The Justice Department today announced the seizure of the largest criminal marketplace on the Internet, AlphaBay, which operated for over two years on the dark web and was used to sell deadly illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals throughout the world. The international operation to seize AlphaBay's infrastructure was led by the United States and involved cooperation and efforts by law enforcement authorities in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, as well as the European law enforcement agency Europol.

On July 5, Alexandre Cazes aka Alpha02 and Admin, 25, a Canadian citizen residing in Thailand, was arrested by Thai authorities on behalf of the United States for his role as the creator and administrator of AlphaBay. On July 12, Cazes apparently took his own life while in custody in Thailand. Cazes was charged in an indictment (1:17-CR-00144-LJO), filed in the Eastern District of California on June 1, with one count of conspiracy to engage in racketeering, one count of conspiracy to distribute narcotics, six counts of distribution of narcotics, one count of conspiracy to commit identity theft, four counts of unlawful transfer of false identification documents, one count of conspiracy to commit access device fraud, one count of trafficking in device making equipment, and one count of money laundering conspiracy. Law enforcement authorities in the United States worked with numerous foreign partners to freeze and preserve millions of dollars' worth of cryptocurrencies that were the subject of forfeiture counts in the indictment, and that represent the proceeds of the AlphaBay organization's illegal activities.

On July 19, the U.S. Attorney's Office for the Eastern District of California filed a civil forfeiture complaint against Alexandre Cazes and his wife's assets located throughout the world, including in Thailand, Cyprus, Lichtenstein, and Antigua & Barbuda. Cazes and his wife amassed numerous high value assets, including luxury vehicles, residences and a hotel in Thailand. Cazes also possessed millions of dollars in cryptocurrency, which has been seized by the FBI and the Drug Enforcement Administration (DEA).

According to publicly available information on AlphaBay prior to its takedown, one AlphaBay staff member claimed that it serviced over 200,000 users and 40,000 vendors. Around the time of takedown, there were over 250,000 listings for illegal drugs and toxic chemicals on AlphaBay, and over 100,000 listings for stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms and fraudulent services. Comparatively, the Silk Road dark web marketplace, which was seized by law enforcement in November 2013, had reportedly approximately 14,000 listings for illicit goods and services at the time of seizure and was the largest dark web marketplace at the time.

"This is likely one of the most important criminal investigations of the year – taking down the largest dark net marketplace in history," said Attorney General Jeff Sessions. "Make no mistake, the forces of law and justice face a new

challenge from the criminals and transnational criminal organizations who think they can commit their crimes with impunity using the dark net. The dark net is not a place to hide. The Department will continue to find, arrest, prosecute, convict, and incarcerate criminals, drug traffickers and their enablers wherever they are. We will use every tool we have to stop criminals from exploiting vulnerable people and sending so many Americans to an early grave. I believe that because of this operation, the American people are safer – safer from the threat of identity fraud and malware, and safer from deadly drugs.”

“Transnational organized crime poses a serious threat to our national and economic security,” said Acting Director Andrew McCabe of the FBI. “Whether they operate in broad daylight or on the dark net, we will never stop working to find and stop these criminal syndicates. We want to thank our international partners and those at the Department of Justice, the DEA and the IRS-CI for their hard work in demonstrating what we can do when we stand together.”

“The so-called anonymity of the dark web is illusory,” said Acting Administrator Chuck Rosenberg of the DEA. “We will find and prosecute drug traffickers who set up shop there, and this case is a great example of our commitment to doing exactly that. More to come.”

“AlphaBay was the world’s largest underground marketplace of the dark net, providing an avenue for criminals to conduct business anonymously and without repercussions,” said Chief Don Fort of IRS-CI. “Working with our law enforcement partners – both domestically and abroad – IRS-CI used its unique financial and cyber expertise to help shine a bright light on the accounts and customers of this shadowy black marketplace, and we intend to continue pursuing these kinds of criminals no matter where they hide.”

“This ranks as one of the most successful coordinated takedowns against cybercrime in recent years,” said Executive Director Rob Wainwright of Europol. “Concerted action by law enforcement authorities in the United States and Europe, with the support of Europol, has delivered a massive blow to the underground criminal economy and sends a clear message that the dark web is not a safe area for criminals. I pay tribute to the excellent work of the United States and European authorities for the imaginative and resourceful way they combined their efforts in this case.”

AlphaBay operated as a hidden service on the “Tor” network, and utilized cryptocurrencies including Bitcoin, Monero and Ethereum in order to hide the locations of its underlying servers and the identities of its administrators, moderators, and users. Based on law enforcement’s investigation of AlphaBay, authorities believe the site was also used to launder hundreds of millions of dollars deriving from illegal transactions on the website.

An investigation conducted by FBI Atlanta and the U.S. Attorney’s Office in the Northern District of Georgia identified an AlphaBay staffer living in the United States. That investigation is ongoing.

The investigation into AlphaBay revealed that numerous vendors sold fentanyl and heroin, and there have been multiple overdose deaths across the country attributed to purchases on the site.

According to a complaint affidavit filed in the District of South Carolina against Theodore Vitality Khleborod and Ana Milena Barrero, an investigation into an overdose death on February 16, in Portland, Oregon, involving U-47700, a synthetic opioid, revealed that the drugs were purchased on AlphaBay from Khleborod and Barrero. According to another complaint affidavit filed in the Middle District of Florida against Jeremy Achey, an investigation into a fentanyl overdose death in Orange County, Florida, on February 27, revealed that the lethal substance was purchased on AlphaBay from Achey.

Charges contained in an indictment and/or complaint are merely allegations, and the defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

This operation to seize the AlphaBay site coincides with efforts by Dutch law enforcement to investigate and take down the Hansa Market, another prominent dark web market. Like AlphaBay, Hansa Market was used to facilitate the sale of illegal drugs, toxic chemicals, malware, counterfeit identification documents, and illegal services. The administrators of Hansa Market, along with its thousands of vendors and users, also attempted to mask their identities to avoid prosecution through the use of Tor and digital currency. Further information on the operation against the Hansa Market can be obtained from Dutch authorities.

The operation to seize AlphaBay's servers was announced by Attorney General Jeff Sessions; Deputy Attorney General Rod Rosenstein; Acting Assistant Attorney General Kenneth A. Blanco of the Justice Department's Criminal Division; U.S. Attorney Phillip A. Talbert for the Eastern District of California; Acting Director Andrew G. McCabe of the FBI, Acting Administrator Chuck Rosenberg of the DEA and Europol Executive Director Robert Mark Wainwright.

The case is being investigated by the FBI including FBI Sacramento Field Office and DEA, with substantial assistance from the IRS-CI. U.S. Immigration and Customs Enforcement's Homeland Security Investigations also assisted in the investigation. The case against Cazes was prosecuted by Assistant U.S. Attorneys Paul A. Hemesath and Grant B. Rabenn of the U.S. Attorney's Office for the Eastern District of California, and Trial Attorneys Louisa K. Marion and C. Alden Pelker of the Criminal Division's Computer Crime and Intellectual Property Section. Substantial assistance was provided by the Department of Justice's Office of International Affairs and Special Operations Division. Additionally, the following foreign law enforcement agencies provided substantial assistance in the operation to seize AlphaBay's infrastructure: Royal Thai Police, Dutch National Police, Lithuanian Criminal Police Bureau (LCPB), Royal Canadian Mounted Police, United Kingdom's National Crime Agency, Europol, and French National Police.

---

**Attachment(s):**

[Download alphabay-cazes\\_forfeiture\\_complaint.pdf](#)

[Download alphabay-cazes\\_indictment\\_redacted.pdf](#)

[Download alphabay\\_seizure\\_page.pdf](#)

**Topic(s):**

Opioids

Cyber Crime

Drug Trafficking

**Component(s):**

[Criminal Division](#)

[Office of the Attorney General](#)

[USAO - California, Eastern](#)

**Press Release Number:**

17-803

*Updated December 11, 2017*